CYBER MISSION ASSURANCE: A GUIDE TO REDUCING THE UNCERTAINTIES OF OPERATING IN A CONTESTED CYBER ENVIRONMENT

GRADUATE RESEARCH PROJECT

Michael D. Pritchett, Major, USAF

AFIT/ICW/ENV/12-J01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/ICW/ENV/12-J01

CYBER MISSION ASSURANCE: A GUIDE TO REDUCING THE UNCERTAINTIES OF OPERATING IN A CONTESTED CYBER ENVIRONMENT

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cyber Warfare

Michael D. Pritchett

Major, USAF

June 2012

AFIT/ICW/ENV/12-J01

CYBER MISSION ASSURANCE: A GUIDE TO REDUCING THE UNCERTAINTIES OF OPERATING IN A CONTESTED CYBER ENVIRONMENT

Michael D. Pritchett

Major, USAF

Approved:

Michael R. Grimaila, PhD, CISM, CISSP (Chairman) — 30 MAY 12 Date

Robert F. Mills, PhD (Member) — 30 MAY 12 Date

Abstract

Military organizations have embedded Information and Communication Technology (ICT), collectively known as "Cyberspace," into their core operational processes across all levels of military operations. Cyber mission assurance is an essential risk management activity focused on assuring an organization's mission capability in response to any loss or degradation of cyber capabilities. The cyber mission assurance process requires an in depth analysis of the organization's mission including enumeration of its core mission processes, prioritization of mission processes, mapping of mission processes to underlying cyber capabilities, and application of control measures to mitigate risks to mission capability. Unfortunately, the structure of military organizations makes this type of analysis challenging as the mission tasks and cyber ICT capabilities virtually always span multiple organizational boundaries.

The 24th Air Force recently developed new draft guidance for conducting cyber mission assurance, *24th Air Force & 624th Operations Center Mission Assurance Operating Concept,* 2011. The goal of this research is to present a methodology enabling mission owners to efficiently prepare for cooperative cyber mission assurance engagements with 24th Air Force. The proposed methodology incorporates the new 24th Air Force guidance; best practices from commercial, governmental, and military organizations; and incorporates operational lessons learned. Application of the proposed methodology will enable more efficient and productive cyber mission assurance engagements with 24th Air Force.

Acknowledgments

I would like to express my great appreciation to my research advisor, Dr. Michael R. Grimaila, for his insight and support throughout the writing of this document. The insightful discussions from his experience on the topic of this project were very timely and thought provoking. Thank you for taking me on as a research student.

I would also like to express my sincere gratitude and appreciation to MSgt Patrick Patterson of 24th Air Force. His subject matter expertise on this research topic was invaluable to the completion of this project. Thank you for putting up with my many phone calls and questions.

I am truly indebted to my wife and son for putting up with me during my career thus far and school this last year. Without their loving support, I would not have made it this far.

Maj Michael D. Pritchett

Table of Contents

Page

Page

List of Figures

List of Tables

Table Page

CYBER MISSION ASSURANCE:
A GUIDE TO REDUCING THE UNCERTAINTIES
OF OPERATING IN A CONTESTED CYBER ENVIRONMENT

I. Introduction

The United States Air Force (USAF) has its roots buried deeply in the use of technology to enhance its mission capabilities and effectiveness. From the all important Norden bombsight used during the early days of the Army Air Corps in World War II, to the laser guided munitions of the Vietnam Era, the Conventional Air Launched Cruise Missiles of the first Gulf War, the use of B-2 Stealth Bombers in Operation Allied Force and the GPS-aided Joint Direct Attack Munitions used in Operations Enduring and Iraqi Freedom, the Air Force mission is very dependent upon technology. Technology has dramatically changed the Air Force from a mentality in Billy Mitchell's day of sending a multitude of bombers loaded with dozens of bombs to cover just one target due to inaccurate weapons and aircraft survivability concerns, to one bomber loaded with dozens of smart weapons to cover multiple targets due to improved precision and defensive technologies.

Today, the success of virtually every military operation is dependent upon the availability, quality, and quantity of information communicated in and through Information and Communication Technology (ICT), collectively known as "Cyberspace." The increasing dependence upon ICT has resulted in an environment where the loss or degradation of the availability, confidentiality, or integrity of a cyber resource or

information flow can result in significant mission degradation or failure (Ware, 1970; GAO, 1996; Jajodia, Ammann, & McCollum, 1999; Fortson & Grimaila, 2007). It is therefore of no wonder why there is a significant emphasis placed on cyberspace operations in the Department of Defense (DoD) and Air Force, second only to nuclear programs. Organizations typically address this type of risk through an introspective, enterprise-wide focused risk management program that continuously identifies, prioritizes, and documents risks so an economical set of control measures (e.g., people, processes, technology) can be selected to mitigate the risks to an acceptable level. However, this can be challenging for military organizations as their mission objectives often span multiple organizational units, services, and agencies.

Background

The Air Force and the DoD have become ever more reliant on cyberspace assets to perform their missions. The connectivity within the DoD across, between, and within each service and agency has increased drastically to the point of work comes to a stop if cyber resources become unavailable. This leads to the key priorities of cyber focused units such as 24th Air Force (24 AF) and USCYBERCOM: cyber mission assurance. At first glance, cyber mission assurance sounds more like ensuring email and Internet/Intranet connectivity, but it is more about assuring any mission dependent upon the use of cyberspace. It is for this reason that it is imperative that units understand their cyber dependencies. This is essential knowledge that entities like 24 AF and USCYBERCOM need to help assure an organization's mission success.

Purpose and Scope

The purpose of this research is to present a methodology to enable unit commanders to efficiently prepare for cooperative cyber mission assurance engagements with 24 AF. This research effort discusses guidance from 24 AF; reviews best practices from commercial, governmental, and military organizations; and considers lessons learned from the operational environment to provide the reader both with an overall understanding of cyber mission assurance and a means to efficiently interact with 24 AF when building cyber mission assurance plans. The work presented will help to guide a unit in the process of determining mission to critical cyber asset lists that are prioritized and how to engage with 24 AF to develop a plan for cyber mission assurance. Lastly, the project will look to help reduce the uncertainties of operating in a contested cyber environment by making suggestions on ways to exercise cyber mission assurance.

This project was scoped based on the author's more than 13 years experience in B-52H bomber operations in a high assurance environment and offers a framework for discussion on which the author can speak intelligently and confidently. The intent is to use this experience to enable creation of practical examples for the sake of discussion but generic enough for units of any type (aircraft operations, maintenance, logistics, etc) to use this project as a resource to enable cyber mission assurance within their respective units.

It is also important to note this research will deal mainly with one key aspect of cyber mission assurance: prioritized mapping of critical missions to cyber assets. There are other aspects of mission assurance that will not be covered as they are far more technical in nature and therefore outside the scope of this particular project.

Organization

The research for this project was divided into three parts that build on each other. The first part is in Chapter II, which discusses why a unit commander should care and be proactive when it comes to cyber mission assurance. The discussion will look at the definition of cyber mission assurance to better understand why it is not just a cyber unit's problem. Lastly, this chapter will show that the unit needs to be proactive, as cyber mission assurance will not just happen.

Chapter III will look at how a unit can be better prepared to engage 24 AF in developing a mission assurance plan. Going in a little more prepared to engage 24 AF with a prioritized mapping of critical mission sets to critical cyber assets will decrease the amount of time needed to develop a cyber mission assurance plan.

Reducing the uncertainties of operating in the contested environment will be the focus of Chapter IV. What good is a plan if it is never tested before the big game actually happens. There is not a sports team that takes the field of battle on game day without having practiced the plan of attack. This chapter will emphasize the importance of exercising these plans by giving suggestions for what and how to exercise as well as what the end state goals of an exercise plan should be.

II. Understanding Cyber Mission Assurance

To understand the importance and relevance of the methodology presented in this project, there must be a discussion on what cyber mission assurance is and why it is important for a unit commander to proactively engage 24 AF with its cyber mission assurance needs. This section will first review the different definitions of cyber mission assurance found during research for this project. Next, motivated by these definitions, this author will look to show cyber mission assurance is not just 24 AF's task to deal with and therein finally show the need for unit commanders to be proactive when engaging 24 AF.

What is Cyber Mission Assurance

Research on the topic of cyber mission assurance showed only one general definition for mission assurance in a DoD Directive for critical infrastructure. There is a definition for cyber mission assurance found in Air Force Doctrine documents. Of the other documents researched, writers break apart the terms mission and assurance and delve into the definition of these terms separately to derive a definition for use in their respective writings, most writers leaving out the term cyber all together. This being the case, this section will mention a few of these definitions as well as what is written in some of the DoD, Joint and USAF publications. These definitions will serve as background to influence later discussion on the importance of the unit commander to be proactive as it pertains to cyber mission assurance as well as set the stage for the methodology to be described in Chapter III of this project.

Grimaila et al. took the approach of defining the terms mission and assurance separately and then bringing the terms together to have a common ground for the rest of the paper (Grimaila, Mills, Haas, & Kelly, 2010). The authors used the definition of "mission" from Joint Publication (JP) 1-02 "Department of Defense Dictionary of Military and Associated Terms", stating:

1. *The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore,*
2. *In common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task,*
3. *The dispatching of one or more aircraft to accomplish one particular task (Department of Defense, 2011a).*

The authors further break the definition down to discuss three different types of tasks to accomplish in order to complete the mission which are linked through objectives and effects as spelled out in JP 5-0, "Joint Operation Planning": specified, implied and essential tasks (Department of Defense, 2011c).

Table 1 Mission Tasks

Specified Tasks	In the context of joint operation planning, a task that is specifically assigned to an organization by its higher headquarters.
Implied Tasks	In the context of joint operation planning, a task derived during mission analysis that an organization must perform or prepare to perform to accomplish a specified task or the mission, but which is not stated in the higher headquarters order.
Essential Tasks	A specified or implied task that an organization must perform to accomplish the mission that is typically included in the mission statement.

The authors point out that missions can be broken into tasks and most, if not all, of these tasks may be critical for mission accomplishment and may also have cyber dependencies. Grimaila et al. used a definition of "assurance" from the American Heritage Dictionary:

> *1. A statement or indication that inspires confidence*
> *2. a. Freedom from doubt; certainty about something*
> *b. Self-confidence*
> *3. Chiefly British Insurance, especially life insurance (American Heritage Dictionary, 2011).*

From this definition, the authors defined "assurance" for the context of the paper as that of "reducing the uncertainty in the expected outcome of an activity", specifically relating assurance to risk, "the effect of uncertainty on objectives" (International Organization for Standardization, 2009). Combining the definitions above, they were able to explain mission assurance as "reducing uncertainty in the belief of the organization's ability to successfully complete its mission."

Another group of researchers presented a paper at the 2010 IEEE Second International Conference for Social Computing titled "Managed Mission Assurance: Concept, Methodology and Runtime Support." Within this report the authors pose a very simplistic definition for mission assurance:

> *"…the guarantee that Mission Essential Functionality (MEF) is continued despite partial failures or changes in the system and its operating environment (Pal, Rohloff, Atighetchi, & Schantz, 2010)."*

The above definition, while simplistic and relevant to the authors' paper, makes mention of functionality as opposed to assuring missions and tasks. This is just one of several definitions found during research that shows no clear consensus on the definition of mission assurance, that many times definitions are derived in order to motivate the author's paper.

When looking through the various DoD Joint Publications, there is no definition for mission assurance, much less cyber mission assurance. In JP 1-02 and JP 3-13, *Information Operations*, information assurance is the closest definition to cyber mission assurance found in DoD Joint Publications:

> *"**information assurance** – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities* (Department of Defense, 2006; Department of Defense, 2011a)*."*

While this definition mentions protecting and defending information and information systems it does not mention protecting and defending missions.

As mentioned before, only one DoD definition could be found for the term "mission assurance" and it was in the *DoD Policy and Responsibilities for Critical Infrastructure*, DoD Directive 3020.40:

> *"**mission assurance**. A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the Department of Defense to carry out the National Military Strategy. It links numerous risk management program activities and security-related functions, such as force protection; antiterrorism; critical infrastructure protection; IA; continuity of operations; chemical, biological, radiological, nuclear, and high explosive defense; readiness; and installation preparedness to create the synergy required for the Department of Defense to mobilize, deploy, support, and sustain military operations throughout the continuum of operations. (Department of Defense, 2010)."*

This definition of mission assurance is not just tied to cyber, but other areas as well. But the definition does build a foundation for mission assurance in cyberspace to allow for

the mobilization, deployment, support and sustainment throughout all phases of military operations.

Research done through Air Force publications revealed a definition of cyber mission assurance in AFDD 1, *Air Force Basic Doctrine*, and AFDD 3-12, *Cyberspace Operations*. Both documents define cyber mission assurance as:

> ***"mission assurance (cyberspace)****. Measures required to accomplish essential objectives of missions in a contested environment. Mission assurance entails prioritizing mission essential functions, mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities (Department of the Air Force, 2010)."*

This definition relates closely to cyberspace and spells out some specific tasks (not necessarily all inclusive) that need to be accomplished to provide mission assurance: prioritizing mission essential functions, mapping mission dependence on cyberspace, identifying vulnerabilities and mitigating risk of known vulnerabilities.

Mission Assurance – Not Just 24th Air Force's Problem

Mission assurance is ultimately the commander's responsibility and undoubtedly is something thought about by commanders at all levels but not necessarily codified on paper. It may be thought more in the light of Operational Risk Management (ORM) but this is more often related to the risks of safely performing a mission and less to the risks to mission accomplishment. With cyberspace being more global than a local engagement within an AOR, the vast number of cyber dependencies that need to be monitored means cyber mission assurance cannot be left to thoughts on mission assurance in a commander's mind, mission owners need to codify mission tasks and cyber dependencies for those tasked with cyber mission assurance.

There were two statements found during research that drive home the level of importance placed on cyber mission assurance by senior leadership, first by Mr. Robert F. Lentz, Deputy Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance, before the U.S. House of Representatives Armed Services Committee Subcommittee on Terrorism, Unconventional Threats & Capabilities on 5 May 2009 where he quoted the Department of Defense's Guidance of the Deployment of the Force (GDF) for 2010-2015:

> *"All DoD Components will reduce the risk of degraded or failed missions by developing doctrine/tactics, techniques and procedures and planning for, implementing, and regularly exercising the capability to fight through cyber or kinetic attacks that degrade the Global Information Grid (Lentz, 2009)."*

The second comes from the Department of Defense Strategy for Operating in Cyberspace, which makes reference to cyber mission assurance in "Strategic Initiative 1: DoD will treat cyberspace as an operational domain to organize, train and equip so that DoD can take full advantage of cyberspace's potential":

> *"Operating with a presumption of breach will require DoD to be agile and resilient, focusing its efforts on mission assurance and the preservation of critical operating capability (Department of Defense, 2011b)."*

These two statements make it appear to be just a 24 AF problem. A case can be made for why it is as much a problem for a unit commander as it is for 24 AF.

Billy Mitchell saw how aircraft technology would change the way we fight wars. While he may not have been able to imagine it then, there is no doubt that ICT have taken the Army Air Corps. from those days of sending 10-20 bombers to attack one target, to today's Air Force sending one bomber to cover 10-20 targets. Computers and cyberspace

have made the Air Force more efficient in training and fighting, from Link-16, to the aircraft systems that target GPS aided Joint Direct Attack Munitions, to remotely piloted aircraft operated from half a world away. So much so, the Air Force and the other sister services have become even more dependent on cyberspace as the DoD draws down in forces and budgets, forcing all the services to do more with less.

From this author's experiences in the B-52 community as a Weapons School Graduate, a mission planner and an assistant director of operations of an operations support squadron in the Air Force's largest bomber wing, it is easy to see the intertwining of cyberspace and B-52 operations, or any unit for that matter. In the day-to-day home station environment, accomplishing the daily duties around a squadron comes to a stand-still when the network becomes unavailable. While flying operations may continue, it is not without much angst as things such as flight schedules, lists of currencies and aircraft maintenance information (just to name a few) are located on the network. Other mission support tasks such as intelligence and weather support become harder to accomplish if access to the Internet is down. While operations might not stop entirely, operations tempo definitely may slowdown.

Looking at wartime operations, the damage becomes more significant. With technology driving a lot of the B-52's arsenal, having key systems or connections go down could keep a unit from accomplishing the mission as directed. There are certain systems that if knocked off-line, could prevent certain weapons from being planned/programmed for maximizing weapon reliability and survivability, thus sacrificing effectiveness as tasked by the Joint/Combined Forces Air Component Commander through the Air Tasking Order (ATO). In order to mitigate such a problem,

the mission planning system is typically set up to allow mission planners to operate "disconnected" from cyberspace. While this kind of setup keeps mission planners relatively safe from cyber attacks or degradations, it does not take advantage of certain efficiencies of being "connected" to cyberspace, like up-to-date data and systems which becomes manual and, most often, time consuming in nature. This does not mean that mission planners do not need connectivity, as threat orders of battle, ATOs and targeting data (again to name a few) are distributed electronically via Secret Internet Protocol Router Network (SIPRNet). Typically units are geographically separated from the Air Operations Center (generally by at least a thousand miles), making it a challenge for distributing the needed electronic files when SIPRNet is down or degraded. Add to this, the beyond line of sight communication links used to pass targeting information in-flight well before entering the area of responsibility could further affect mission effectiveness in a degraded or denied cyber environment.

This is just one airframe or unit of many having cyber dependencies that could result in critical mission failure if not able to operate in a degraded or denied cyber environment. One of the biggest challenges facing 24 AF is the ability to map out a prioritized list of the massive number of missions out there with critical cyber dependencies. This was made evident from out-brief slides from the Military Operations Research Society (MORS) symposium on Mission Assurance: Analysis for Cyber Operations Special Meeting, when Working Group 3 (which included representation from 24 AF and USCYBERCOM) recognized the need for identifying critical missions and assets and mapping critical assets to missions to aid in mission assurance (Military Operations Research Society, 2011a, p. 28). In themes across the working groups, it was

determined that “Mission Assurance requires an understanding of how network capabilities map into the mission” and that “such maps are seldom, if ever, generated (Military Operations Research Society, 2011b).” What is being seen is a lack of quality information that can be used to make prioritization decisions when cyber systems come under a cyber attack. What ends up happening is due to this lack of information, critical systems may inadvertently get locked down/out due to these attacks thus affecting the critical mission that system supports, e.g. mission planners lack the tools/information to plan the mission, when it may have been avoidable.

Confidentiality and integrity of data at rest or in motion is another key aspect of mission assurance. In other words, how is the data used for mission accomplishment protected from prying eyes or from tampering while it is being stored or while it is in transit from one system to another. Many perceive cyber mission assurance as making sure the actual cyber asset is available, what many overlook is the fact cyber assets are typically information storage or transportation devices. The information stored or passed on these systems can go toward the success or failure of the mission if the information is not sufficiently protected in either of its two states, at rest or in motion. On SIPRNet systems, in motion data is typically taken care of due to the bulk encryption techniques (pre-shared cipher keys), unlike NIPR where most everything is passed in the clear with the exception of Secure Socket Layer and Transport Layer Security connections which are still susceptible to man in the middle attacks. But when looking at the storage side of data or data at rest, most often the data is not encrypted or protected from prying eyes or data tampering on either SIPRNet or NIPRNet. What then are the ramifications to mission accomplishment if data used for the mission is somehow compromised? How

can a mission owner be confident the data used for mission accomplishment is good? Therefore, not just the mapping of cyber assets to missions needs to occur but the identification of data flows is also crucial to mission assurance.

One clear conclusion that can be drawn thus far is that cyber mission assurance is not solely a 24 AF problem; it is a mission owner problem. 24 AF cannot adequately map and prioritize network capabilities and data flows to missions without the aid of the mission owners to identify the critical mission tasks. For one, 24 AF does not know the in's and out's of every mission a unit may have and second, they do not have the man power, whether it be number of personnel and/or subject matter experts, to be able to accomplish this task for the entire Air Force. As far as mission owners, it goes towards their mission success, so it would be in the best interest of mission owners to be proactive in making sure the mapping of mission to network is covered and prioritized correctly as well as wanting to ensure the data being stored and transmitted across those systems is adequately protected. Additionally, it will help mission owners to find gaps allowing them to develop contingency plans to enable operations in a degraded or denied environment. This is where 24 AF and maybe even base cyber units will help mission owners create or update the cyber portions of their contingency plans.

Unit Commanders Need to be Proactive

The recent creation of a draft of the *24th Air Force and 624th Operations Center Mission Assurance Concept* has changed how 24 AF is approaching mission assurance. 24 AF will now engage with **requesting** MAJCOMs or COCOMs to build mission assurance plans (24th Air Force, 2011 (DRAFT)). For the most part, 24 AF is not going

out and tracking down all organizations within the Air Force to acquire the information needed to provide mission assurance services, this would be too unmanageable to accomplish and has not worked thus far. In order to provide quality mission assurance services, organizations need to come to 24 AF with their needs in order for mission assurance planners to develop plans.

According to the American Heritage Dictionary Online, one of the definitions of the word "plan" is:

> *"An orderly or step-by-step conception or proposal for accomplishing an objective (American Heritage Dictionary, 2011)…"*

This definition would imply a certain amount of forethought and information gathering as to be able to create a plan for later execution. Therefore, waiting until there is a need for mission assurance in the middle of a conflict, does not a plan make nor does it make for a successful conflict. 24 AF has recognized within the operating concept document that plans could take up to six months to develop (24th Air Force, 2011 (DRAFT)). This is a significant amount of time in which missions could go ineffective due to cyberspace degradations or denials. Therefore, units need to be proactive and engage with 24 AF **now** to start preparing mission assurance plans and to have a chance to exercise those plans prior to operations/conflicts. Now is the time to start building the prioritized mapping of critical missions and tasks of a unit linked to cyber assets used to accomplish those critical missions and tasks, not when the unit is trying to deploy or while in the middle of the fight.

This chapter presented a few definitions of mission assurance, the importance placed on continuing operations in a degraded or denied cyberspace environment, how mission

assurance is not just 24 AF's problem but a mission owner's problem as well, and stressed the need for unit commanders to be proactive in engaging 24 AF in regards to mission assurance planning. The next chapter will examine how to best prepare to engage 24 AF in developing mission assurance plans.

III. Research Methodology

In order to successfully engage 24 AF concerning cyber mission assurance, a unit must be reasonably prepared to answer questions concerning missions and mission tasks and how these mission tasks are reliant on cyberspace assets. This chapter will focus on the collection of initial unit mission set(s) data in order to have a successful engagement with 24 AF on building a mission assurance plan. The first section will deal with who should be initiating and completing the mission to cyber asset mapping process. The second section discusses tools and techniques for collecting and compiling data in a coherent manner to aid in the start of the mission analysis phase 24 AF will first perform. The next section deals with determining the unit's mission sets, breaking these mission sets into mission tasks, and mapping out a battle rhythm for a given mission set. The fourth section analyzes the information gathered about the mission sets to determine cyberspace dependencies and what information to gather concerning these cyberspace dependencies. The fifth section discusses mapping and prioritizing the mission sets and cyber assets. Finally, the chapter concludes with how to begin the engagement with 24 AF.

Getting Started

Up to this point, the unit has been the focus of discussion but what will become more apparent in a later section of this chapter is: once a mapping is generated it will need to be routed through the Major Command (MAJCOM) or Combatant Command (COCOM) to get to 24 AF. This leads to an issue that needs to be mentioned up front of who should be initiating and completing the mission to cyber asset mapping process. In the case of

the COCOM, while they may recognize the need for cyber mission assurance for a given unit's mission set, they have no in depth insight into the inner workings of a unit's mission sets and mission tasks to create such a mapping and, therefore, would be handing the dirty work of creating the mission to cyber asset mapping down to the mission owner for completion.

The MAJCOM, however, may have sufficient subject matter experts (SMEs) on hand to both initiate and at least begin to create the mapping. The advantage of the MAJCOM taking the "wheel" is that the product can be tailored to work across multiple units of the same mission function, e.g. Air Force Global Strike Command (AFGSC) putting together a mapping of mission sets for both B-52 wings, the 5th Bomb Wing in North Dakota and the 2d Bomb Wing in Louisiana. But it may be in the best interest of the MAJCOM, if they are the initiator of the mapping process, to be a coordinator between multiple units to allow the units to develop a mutual mapping of mission to cyber assets since the units are closest to the mission and provide the in depth look into tasks and cyber assets that the MAJCOM may not have.

If a unit were to initiate the mapping process and there is a community of geographically collocated or separated units under a MAJCOM with the same mission function, similar to the B-52 example given in the previous paragraph, then it would be in the best interest of that community for the units to work together. This would provide the MAJCOM with a mutual mapping to present to 24 AF as a part of the cyber mission assurance request for support document discussed later in this chapter.

For the remainder of this chapter, the term “unit” refers to the entity, whether it be a specific unit, MAJCOM or COCOM, who actually is putting the information together to develop the mission to cyber asset mapping.

Tools and Techniques

To facilitate the collection and consolidation of mission sets, mission tasks and cyber assets, a brief discussion of tools and techniques for collecting and consolidating such data is important. First, this section will look at the *Department of Defense Architecture Framework Version 2.0* (DoDAF V2.0), Systems Viewpoint-5 (SV-5) Model as a model for collecting and consolidating the data. Then, this section will describe the types of information concerning cyber assets that need to be collected from Donald L. Pipkin’s book, *Information Security: Protecting the Global Enterprise* (Department of Defense, 2009; Pipkin, 2000)

DoDAF V2.0 - SV-5

DoDAF V2.0 “serves as the overarching, comprehensive framework and conceptual model enabling development of architectures (Department of Defense, 2009)” within the DoD. This document provides a means for developing and modeling a system architecture that ties functions or objectives to systems and system processes using a common format that is understandable across different agencies within the DoD. The document has many different views or models that can be tailored to capture the information that is trying to be conveyed or transferred. Therefore, the document is not purely prescriptive in nature.

Of the many models that could be used, it was suggested through contacts at 24 AF that a Systems Viewpoint - 5 would be a useful model to follow for providing needed mission and system data. Within DoDAF there are two different models for SV-5, an SV-5a and SV-5b. The SV-5a model is an Operational Activity to Systems Traceability Matrix with the important role of tracing system function requirements to associated user requirements (Department of Defense, 2009). This and the other models are intended for use in building user systems but using the SV-5a model as a guide for mapping missions to cyber assets makes it a very useful tool for gathering the needed information for the start of developing mission assurance plans. Useful information that can be gathered is:

- Tracing functional system requirements to user requirements
- Identification of overlaps or gaps (Department of Defense, 2009).

In the case of mission assurance, system requirements are the cyber dependencies and the user requirements are the mission tasks required for mission success or effectiveness. Of note, this model could be used for more than just cyber mission assurance showing missions and cyber dependencies. It could be used to map out a mission's dependencies on other outside agencies or actors that do not fall inside the cyberspace realm, but this is outside the scope of this research project. The SV-5b is essentially the same as the SV-5a but it could be used to summarize the SV-5a and it could be used to take functionality down to the performers executing activation of the function. Based on the research conducted, the SV-5a will be the model of choice for this project.

As previously stated, the models are not prescriptive in nature, meaning there is no defined set of steps nor is there a specific presentation design for collected data, this allows tailoring for the organization's needs. Later in this chapter, a method for

collecting and presenting the data is presented. It is not a 100% solution but one that captures the data necessary to begin planning for cyber mission assurance with 24 AF.

Pipkin's Resource Inventory

The book *Information Security, Protecting the Global Enterprise*, Donald L. Pipkin discusses how to implement information security in an enterprise, breaking it up into five distinct phases: inspection, protection, detection, reaction and reflection. The first critical step in the inspection phase, conducting a resource inventory, will be the basis for collecting cyber asset data later in this chapter.

Within the step of resource inventory, Pipkin suggests an organization should identify all of its cyber related systems to include every end system that touches the network and information on each system's MAC address with a listing of all of the software applications including which applications are mission critical and what internal and external network resources the applications use. While compiling this data on cyber assets, the assigning of ownership of these systems needs to be accomplished to provide accountability so someone can be contacted when remediation or other actions related to the systems needs to occur and for maintaining contingency plans for those systems. Finally, a determination of the value and security classification of the systems should be accomplished which will aid in the prioritization of these systems (Pipkin, 2000).

Enumerating all of a unit's cyber assets would be a daunting task to handle right at first due to the OPSTEMPO of the unit and its many competing interests. While enumerating all of a unit's cyber assets may be the ultimate goal for a unit to truly understand all of its cyber dependencies, the methodology in this chapter only has resource inventory occurring after the enumeration of mission sets, tasks, and sub-tasks.

This will focus a unit's limited and strapped resources on the more important mission critical cyber assets.

Automated Methods

As mentioned there is no one technological solution to aid in the collection of the mission tasks and cyber dependencies. However there is much work being done on finding the technological solution for mission assurance mapping and monitoring but it is not yet fielded as it is a difficult process. D'Amico et al. present scenarios in order to continue research into development of an automated mission impact system, Cyber Assets to Mission and Users (Camus). Haigh et al. is working on a project called the Automated Intelligent Management for Integrated Strategy and Tactics (AIMFIRST) which is an approach to providing automated mission assured networking, involving modeling missions using mission planner inputs and adapting network discovery and modeling tools. While not all inclusive, these are some of the ongoing research into automating mission assurance mapping and impact assessment.

Determine Mission Sets

Every unit has at least one mission and in the case of some flying units, some have many different types of missions a unit could be tasked to perform based on the capabilities of the tasked Mission Design Series (MDS). In the case of many mission sets, these mission sets may have similar tasks that are performed with slight variances on the mission set. The goal of this section is to provide a methodology for determining the unit's mission sets, delineating the tasks and sub-tasks for each mission and then mapping out the battle rhythm for when these tasks are performed. In order to provide clarifying

examples, this report will pull from the author's experience gained in B-52H operations. This in no way limits the implementation of this methodology to just flying or other operations oriented organizations.

Work Most Critical to Least Critical Missions

The first task for a unit is to list all of the missions or mission sets the unit could be or are tasked to accomplish. For an aircraft maintenance unit, it could be as generic as providing mission capable aircraft for the flying unit to perform ATO assigned missions. For a flying unit, generally speaking it might be a strategic attack sortie but more specifically a long range strike sortie with a specific weapons load-out that has some significant planning and execution implications say standoff cruise missiles.

This step is a high level look and should not be getting into the detailed tasks of each mission set but more to parse out the different missions to determine where to focus efforts. These missions/mission sets may include both contingency/war-time and peace-time missions. In this case, a prioritization would need to occur to continue to focus efforts. Since, contingency/war-time mission sets can carry higher implications in regards to mission failure, time should be mostly spent on these types of missions in the beginning. Then as time allows and the war-time missions have mission assurance plans created, later revisiting peace-time operations could be in order.

Focusing on the war-time/contingency mission sets, an attempt needs to be made in prioritizing the missions before moving on to the next step of delineating tasks and sub-tasks for each of the missions in order to focus on the most important missions first and work down through the list. Prioritizing may be difficult if doing this analysis in a peace-time environment since mission priority often times comes from the commander's

intent and/or the ATO in a war-time/contingency environment. In this case, it might be best to choose a mission typically designated as high priority or a frequently tasked mission. Once the onion is peeled back on this mission, many dependencies inside and outside of the unit may be brought to light of which may prove it to be best the candidate for cyber mission assurance planning. For the purposes of further development of the methodology, a generalized mission for the B-52H will be used as an example: strategic attack mission – long range strike with conventional stand-off weapons.

Delineate Tasks and Sub-Tasks for each Mission

Now that missions have been enumerated and a mission task has been selected for continued analysis, the next step is to break the mission down into tasks and sub-tasks. This is where the unit gets down into the weeds of a mission and simply is identifying the individual tasks required for mission accomplishment. A unit needs to enumerate every task and sub-task from beginning to the end of the mission to ensure there are no known open gaps in the plan later. Obviously, every pop-up contingency cannot possibly be considered, but the finer the detail the better as plans are something to deviate from "no plan of operations extends with certainity beyond the first encounter with the enemy's main strength (Moltke & Hughes, 1995)."

Looking at Figure 1, in an Excel spreadsheet format the mission tasks are spelled out. In the first column is a name for the mission task itself, in this case one is "Mission Planning Data Collection". When looking at the mission tasks, if the overall step is too broad it could be broken into sub-tasks to capture the detail of the overall task. For each task or sub-task, a description of the task to include actions taken and who performs the actions, if known, is needed in the description. The third column gives details on internal

information flows, to whom it flows and what information is flowing. The last column continues on the theme of information flows except it is the external side, to whom and what is flowing outside the unit, on and off installation. The more descriptive the better as this will allow mission assurance planners to ask smart questions when they begin to analyze the mapping that is provided. Being as detailed as possible will help later in the section dealing with determining cyber assets as well.

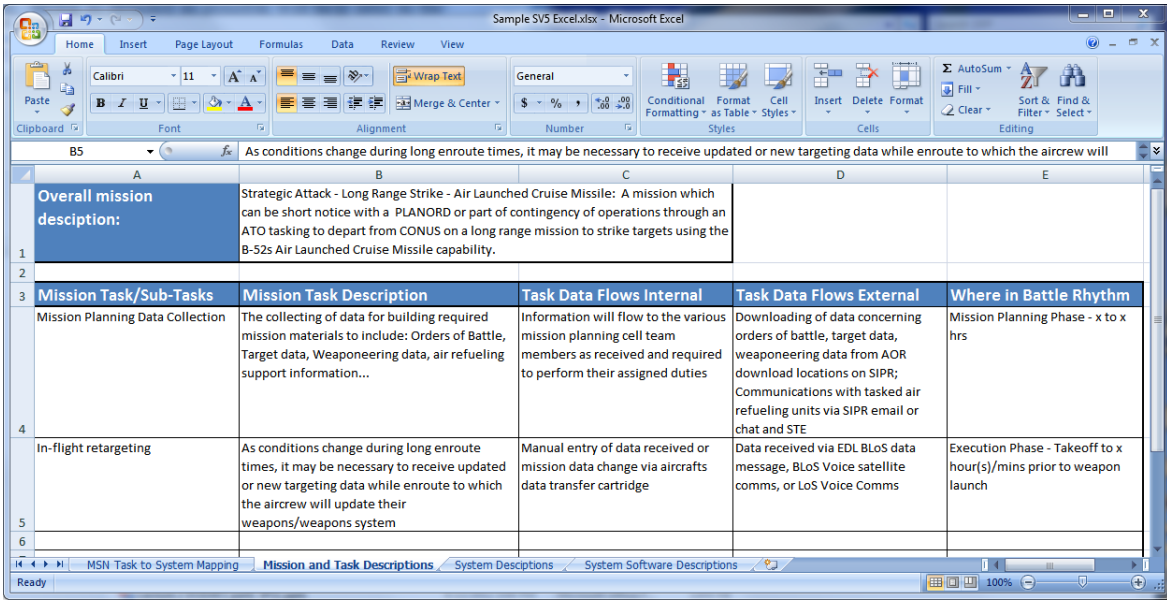


Figure 1 Mission and Task Descriptions

Map out the Battle Rhythm for each Mission

Cyberspace Superiority is defined as "the operational advantage in, through and from cyberspace to conduct operations **at a given time** and **in a given domain** without prohibitive interference (Department of the Air Force, 2011) [emphasis added]." This is very much like the definition of Air Superiority "the degree of dominance that permits friendly land, sea, air, and space forces to operate **at a given time and place** without prohibitive interference by the opposing force (Department of the Air Force, 2011)

[emphasis added]." Not unlike Air Operations, Cyberspace is a large and vast domain in which it is hard to maintain superiority in all places at all times with the limited amount of resources available to today's Air Force. For this reason, 24 AF needs information on the battle rhythm of the mission sets in order to map out those times in which mission assurance is most crucial. When planning in a peace-time environment for contingency or war-time operations, giving as good estimates of time frames for task accomplishment will be beneficial for the initial plan and can be updated when it comes time to implement the plan.

Determine Cyber Assets

Now that the mission is defined and the tasks and sub-tasks enumerated with as much detail as can be provided from the beginning to the end of the mission, analysis can now begin on determining cyber dependencies and enumerating those dependencies.

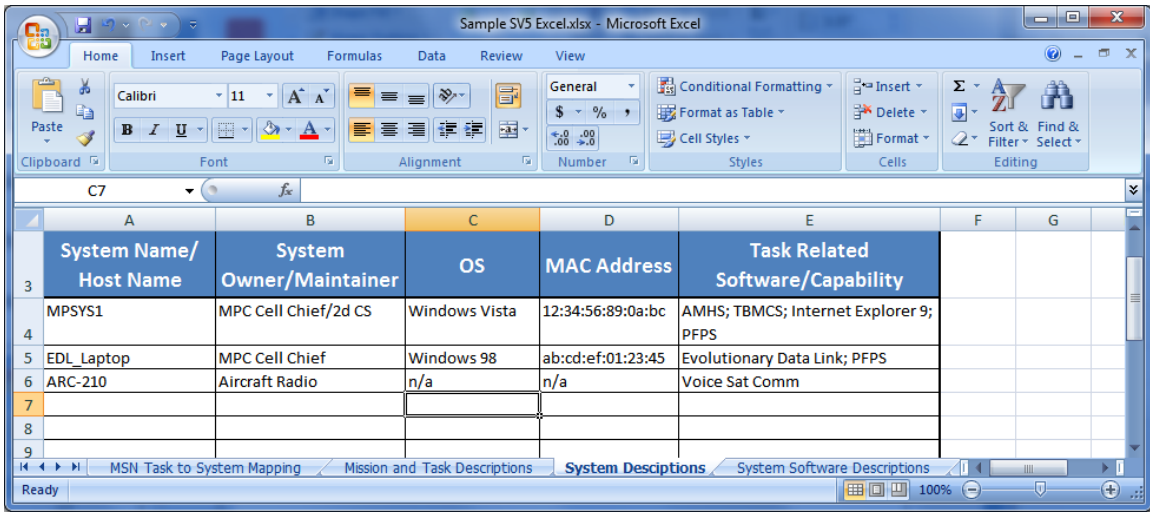
Analyze Tasks to Determine Cyber Dependencies

While enumerating the mission tasks and sub-tasks, some of the analysis to determine cyber dependencies has already started. The task internal and external data flows is a good place to start when determining the cyber dependencies. This is where the analysis turns to how the information is collected, stored and/or disseminated. Analyze each task and determine if the information collected, stored and/or disseminated was accomplished via computer, telephone and/or fax machine, even land mobile radio as these may be transmitted across a network to improve functionality. Including satellite communications, either voice or data, is important as well despite the fact the communications may not touch a network or the Internet, the systems that control the

satellites may need to be considered for mission assurance purposes. Listing other line of sight radios would be mainly for situational awareness purposes to potentially show a redundancy capability.

Enumerate the Cyber Dependencies

Now that there is an idea of the cyber dependencies, data needs to be collected on these cyber dependencies. Collecting the data for the cyber dependencies will take two steps depending on the type of system used, data on the system itself, and data on task related software/applications running on the system. Figure 2 below will continue the B-52H example beginning with the collection of system data.

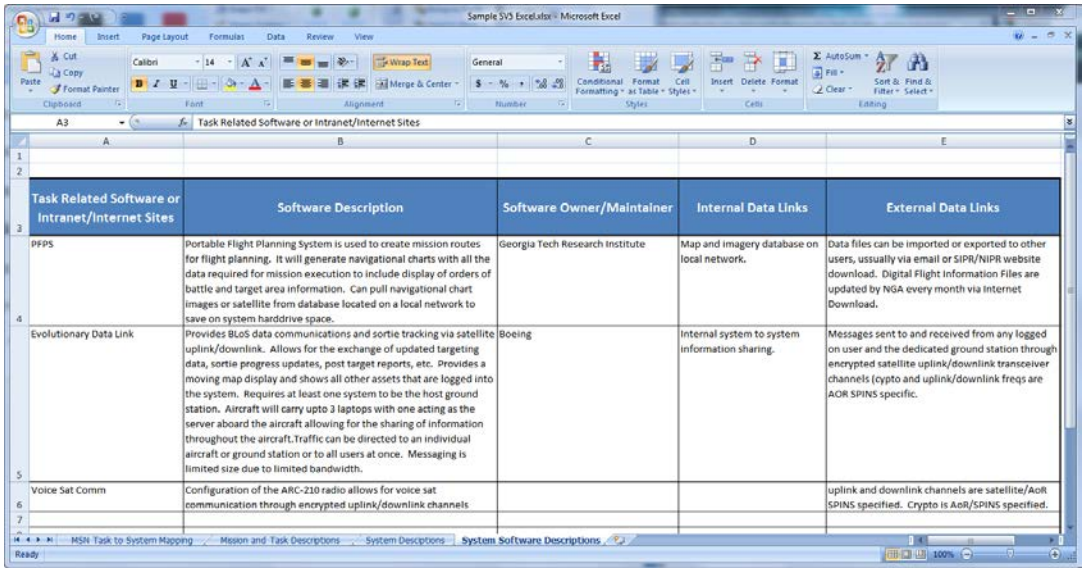


	A	B	C	D	E	F	G
3	System Name/ Host Name	System Owner/Maintainer	OS	MAC Address	Task Related Software/Capability		
4	MPSYS1	MPC Cell Chief/2d CS	Windows Vista	12:34:56:89:0a:bc	AMHS; TBMCS; Internet Explorer 9; PFPS		
5	EDL_Laptop	MPC Cell Chief	Windows 98	ab:cd:ef:01:23:45	Evolutionary Data Link; PFPS		
6	ARC-210	Aircraft Radio	n/a	n/a	Voice Sat Comm		
7							
8							
9							

Figure 2 System Descriptions

A list of cyber related systems descriptions are pulled from the list of mission tasks and sub-tasks as seen in Figure 2. Much of the listed data is what was suggested by Pipkin earlier in this chapter. First things first, the system name or host name is needed. If it is a computer the host name will help to identify the system on the network and offer a better differentiation between similar systems. Use a system name if it is not

necessarily a computer, i.e.: LMR or ARC-210 Radio. Next, it is helpful to list the owner and/or maintainer of the system. This aids in further analysis later by allowing mission assurance planners to engage with the system owner/maintainer when more data is needed and to provide contact information within the plan for when the plan is executed later. Listing of the operating system is key to having some insight into potential vulnerabilities that may already exist with the system and aids in asking the right questions in developing the mission assurance plan. One other piece of identifiable information for a computer system would be the system's Media Access Control (MAC) address, again this can aid in finding and identifying the system while it is on a network. The last item for system level description is listing the task related software/capability. In the case of a computer system, this is a list of software and applications used to accomplish mission tasks. For non-computer systems, it is the capability the system provides for accomplishing a mission task. With the systems listed, the next step is to make a list of the system software descriptions as seen in Figure 3.



Task Related Software or Intranet/Internet Sites	Software Description	Software Owner/Maintainer	Internal Data Links	External Data Links
PFPS	Portable Flight Planning System is used to create mission routes for flight planning. It will generate navigational charts with all the data required for mission execution to include display of orders of battle and target area information. Can pull navigational chart images or satellite from database located on a local network to save on system harddrive space.	Georgia Tech Research Institute	Map and imagery database on local network.	Data files can be imported or exported to other users, ussually via email or SIPR/NIPR website download. Digital Flight Information Files are updated by NGA every month via Internet Download.
Evolutionary Data Link	Provides BLoS data communications and sortie tracking via satellite uplink/downlink. Allows for the exchange of updated targeting data, sortie progress updates, post target reports, etc. Provides a moving map display and shows all other assets that are logged into the system. Requires at least one system to be the host ground station. Aircraft will carry upto 3 laptops with one acting as the server aboard the aircraft allowing for the sharing of information throughout the aircraft.Traffic can be directed to an individual aircraft or ground station or to all users at once. Messaging is limited size due to limited bandwidth.	Boeing	Internal system to system information sharing.	Messages sent to and received from any logged on user and the dedicated ground station through encrypted satellite uplink/downlink transceiver channels (cypto and uplink/downlink freqs are AOR SPINS specific.
Voice Sat Comm	Configuration of the ARC-210 radio allows for voice sat communication through encrypted uplink/downlink channels			uplink and downlink channels are satellite/AoR SPINS specified. Crypto is AoR/SPINS specified.

Figure 3 System Software Descriptions

The system software description list (Figure 3) should include all of the software/capabilities found in Figure 2, System Descriptions. This list should also contain any intranet/Internet sites that may be used in accomplishment of mission tasks. Then a detailed description needs to be provided on how the software, capability, or intranet/Internet site is used for task accomplishment. This will help mission assurance planners to ask smart questions to minimize gaps in the plan. Next, listing the software, capability, or intranet/Internet site's owner/maintainer is useful for mission assurance planners for inquiring about dependencies that may be further down the line. Finally, listing both the internal and external data links is crucial for aiding mission assurance planners in developing the plan. This information will help the planners to understand the linkages and to where to best focus their efforts in the plan. As with listing the software owners/maintainers, the links may point the mission assurance planners dependencies further down the line.

Mapping and Prioritizing

Much of the work of identifying missions, mission tasks, system descriptions and system software descriptions is now accomplished. The next crucial step is to consolidate the information into a single mapped matrix of mission tasks to cyber systems. This section will take a look at the mapping and prioritizing of the data collected.

Mapping

The mapping itself is pretty straightforward. Referencing the sample matrix in Figure 4 on the following page, take a mission task and list the systems and system

software/applications used to accomplish the task as well as when in the battle rhythm the task occurs. All of this information should come straight from the lists completed earlier in the process. One last key piece of information remains for the completion of the mapping, that is prioritization or in this case Mission Capability Code.

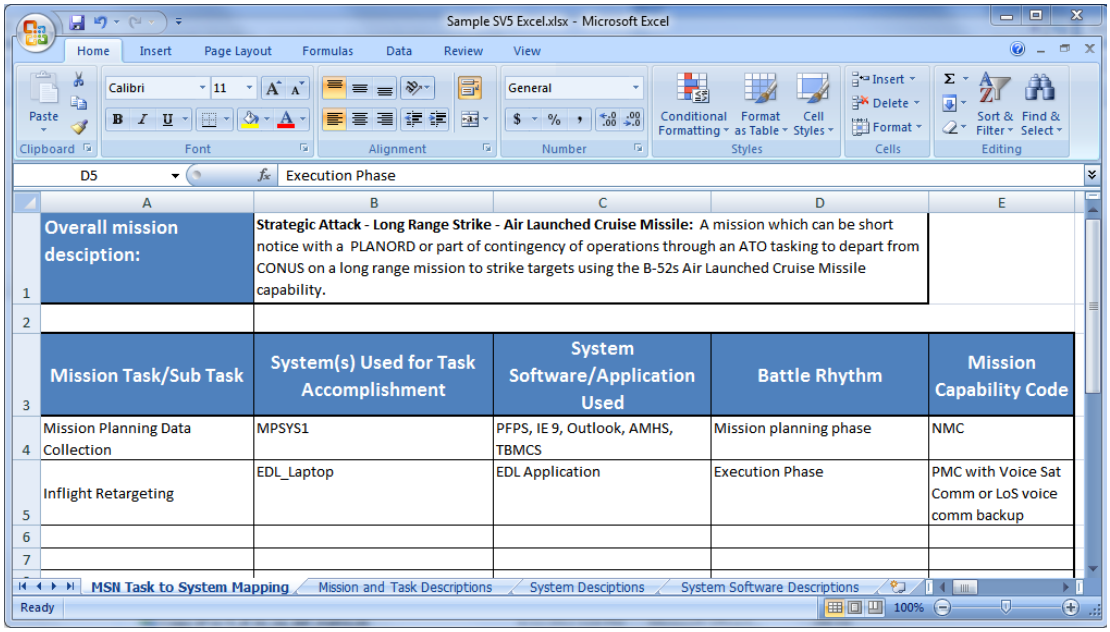


Figure 4 Mission Task to System Mapping

Prioritization

Prioritization in this case is a Mission Capability Code of Full Mission Capability (FMC), Partial Mission Capability (PMC) or No Mission Capability (NMC). These can mean a great many things to many different organizations. Generically speaking for this report they can mean the following:

- **FMC** - Nice to have. Loss of these components will be inconvenient but will not cause mission failure or abort.
- **PMC** - Need to have. Loss of these components may not cause certain mission failure or abort due to potentially having an out of band backup/alternative capability.
- **NMC** - Must have, loss of these components will cause mission to fail or abort; may not have a backup mode of operation.

If the definitions do not meet the organization's needs, the definitions can be tailored to an organization's specific needs or ideas of what FMC, PMC and NMC mean to the organization. As long as they are spelled in clear language, 24 AF can work with the changes. Within the mapping, it is best to provide a listing of the backup or alternative systems for a given task, if there are any.

Thus far, a mapping of mission tasks to cyber assets has been created for one mission set. If there are other missions to break down, the first mapping can serve as a baseline for the rest as it is quite possible there are duplicate or overlapping mission tasks across the different missions. In this case, copying from this baseline and only modifying or adding the differences may speed up the process. It is still important to ensure that each mission is thoroughly analyzed to ensure to the max extent possible that there is nothing left out.

How to Engage with 24th Air Force

The initiation of the engagement with 24 AF will have to be between the MAJCOM's or COCOM's A3 or J3 directorate and 24 AF's A3 directorate. While the bulk of the work of preparing to engage 24 AF on developing a cyber mission assurance plan is completed, there are few more pieces of information that would be useful in the development of the plan:

- CONUS and Forward Operating Locations
- Mission Support Requirements
- Mission C2 Structure

The above information combined with the mission to cyber mapping that was created will allow a unit to be more than adequately prepared to engage 24 AF.

To engage 24 AF a Mission Assurance Request for Support needs to be filled out, the request form can be found in Appendix B of the *24th Air Force & 624th Operations Center Mission Assurance Operating Concept (DRAFT).* It is a template document with certain information needing completion. In the case of "requesting (supported) command or commander", this is the command generating the request for support, the MAJCOM or COCOM. The "specific Mission Assurance set" is the specific mission requested to be supported (24th Air Force, 2011 (DRAFT)).

The third section of the request is the most important, "Desired Effects (Specific)". Based on the mapping of mission tasks to cyber assets, a list of the desired effects can be created. Being as specific as possible when it comes to the asset and mission task to be protected is crucial. Being generic and listing a desired effect of "Ensure the availability of NIPR/SIPR" would not get the desired response, as the point of the whole process is to determine those assets out of the many assets that are most critical to mission accomplishment. Also when creating the list of desired effects, include critical information and information flows that were determined to be critical for mission task accomplishment. Remember, when it comes to cyber assets it is not just about availability, it is also about integrity and confidentiality of information as well.

Once the request is completed, it will be submitted to 24 AF/A3 through the appropriate A/J3 staff equivalent at the MAJCOM or COCOM. 24 AF will then hand it off to the 624 Operations Center (OC) to accept the task of Mission Assurance Support. Once the task is accepted by the 624 OC, it will enter the planning stage where it will enter the Combat Plans Division (CPD) for plan development. During the Mission Assessment and Cyberspace Assessment phases of Mission Assurance plan development,

there will be a continuous back and forth conversation to collect data on mission tasks and cyber dependencies for analysis. Fortunately, most of the delineation of mission tasks and cyber dependencies is already broken out and the analysis by 624 OC will be mostly fine tuning the initial mapping to continue the planning process of cyber threat assessment. During the cyber threat assessment, 624 OC/ISRD will also have to contact the unit's tactics section for the operational view of cyber threats on a kinetic mission, when applicable (24th Air Force, 2011 (DRAFT)).

From here the operations and cyberspace correlation phase assigns operational meaning to each component of the mission architecture so that specific operational impact is immediately understood by those providing mission assurance in the event of a network failure. This leads to capability assessment and coordination, the integration of the threat assessment into the planning process to align capabilities and effects to support the mission (24th Air Force, 2011 (DRAFT)). Once these steps are completed, the formal plan is developed. The next chapter looks at continuing to reduce the uncertainties once the plan is developed.

IV. Reducing Uncertainties

"Thus a victorious army wins its victories first before seeking battle; an army destined to defeat fights in the hope of winning."
– Sun Tzu, The Art of War

At this point there should be a good understanding by the mission owners of their mission sets, mission tasks, and cyber dependent systems. Also, the MAJCOM/COCOM A/J3 has initiated the cyber mission assurance planning process with 24 AF on the behalf the unit. As previously stated, there will be back and forth communication between the mission owner and the 624 OC as they build the plan. Hopefully through the work accomplished prior to engaging 24 AF, the time to completion of the plan has been shortened to well less than the anticipated six months and a plan is established.

During the planning process, there will be much thought given to developing methods to back up those critical functions listed as NMC during the mapping and prioritization phase. These methods may be items the 624 OC will task out via the plan or the methods may be items for which the mission owners need to develop their own contingency plans. In either case, once the measures are put into place they need to be exercised prior to being used in actual combat. This chapter will briefly deal with the importance of exercising, what and how to exercise and finally what the end state goal of exercising should be.

Importance of Exercising

The importance of exercising cannot be understated. While the forces are in a peacetime state is the best time to practice in as accurate and realistic way possible the plans developed for wartime use. In testing these plans, one is able to find what works

and what may not work, as well as catching any items missed in the plan before the actual execution of the developed plan. This leads to increased confidence in the plan. Confidence in knowing the plan has been tested which has most likely led to modifications and additions to the plan, making it more robust to survive first contact with the enemy. Seeing all the parts, pieces and players in a plan work together to solve inefficiencies in the plan (known or unknown) and then revising those plans, can also increase confidence. While all contingencies cannot be planned for nor exercised to, exercising can help to build confidence in the plans and thus reduce the uncertainties of operating in the degraded or denied cyber environment.

What and How to Exercise

The "what" to exercise is probably the most obvious. After the cyber mission assurance plan has been created and on the shelf, the items covered in the plan deemed NMC or most critical for assuring should most definitely be exercised. This also should include any measures suggested by 24 AF that are implemented at the unit level. Items to include in the exercise should also be those that have redundant capabilities in order to ensure the redundant capabilities work as advertised. Probably the most important thing to concentrate on is not only do the planned measures work but to think in terms of the adversary and try to find creative techniques that could be exercised to potentially break the planned measures in an attempt to find missed issues.

The "how" to exercise tends to be a little more difficult. Cyber exercises tend to mainly focus on a cyber unit's ability to defend a small, closed network or "cyber range" to keep from causing problems with operational systems. Such exercises have started

taking place in forums like Red Flag and the U.S. Air Force Weapons School Mission Employment phase, touted as Red Flag on steroids. This makes it difficult to ascertain the effectiveness of a cyber mission assurance plan as, from an operations perspective, the mission owners are not seeing the degradations or denials since the systems are not on the "cyber range". Unfortunately, this will lead to contrived exercise inputs to simulate the degradations/denials of the cyber environment. What is needed is the ability to create a contested environment from which the mission owners can participate to allow the mission owners practice operating in a contested environment and allow 24 AF a method to validate cyber mission assurance plans. Unfortunately this is outside the scope of this research project and is definitely a tough problem to solve.

As mentioned, what are left are contrived exercise inputs to simulate a contested environment. From this author's experience, exercising in a contested cyber environment has not been incorporated into many units' exercises, at least from a mission owner's perspective. Mission owners need to take the next step and start exercising in a simulated contested environment. By accomplishing the mission to cyber asset mapping, a unit can, at the very least, see its cyber dependencies and start incorporating degradation/denial simulations into its local exercises and training to reduce the uncertainties of fighting in the contested environment, ensuring pieces of the cyber mission assurance plan the unit owns work, as well as already identified redundancy capabilities.

End State Goal of Exercising

The ultimate end state goal of exercising should be to reduce the unit's uncertainty of operating in the degraded or denied cyber environment and thus building the unit's

confidence in operating in such a cyber environment. Prior to accomplishing the mission to cyber asset mapping there may have been considerable doubt of a unit's ability to operate in a degraded/denied cyber environment. But once the mission, cyber, and threat assessments are complete, the cyber mission assurance plan is created and other measures are taken, the uncertainties are certainly reduced. Exercising cyber mission assurance plans and measures will further aid in reducing these uncertainties.

Another end state goal would be to find the contingencies missed or inadequately planned for by attempting to break the plan. As seen by this author, when a unit is boxed into a corner during an exercise, that is when the unit becomes the most resourceful in finding new and unique ways to fight out of those tough corners. Exercises should be a forum for encouraging those new and innovative ways to adapt and overcome difficult problems. These problems could be ones never before thought of or it can be tough problems everyone talks about but no one has come up with a workable idea to solve. Exercises should be a breeding ground for solving these types of problems in a consequence free environment, meaning if an attempted solution fails, there is less fear of consequence or reprimand.

Exercising will go a long way in helping to reduce the uncertainties of operating in a contested cyber environment. Exercises can aid in validating 24 AF developed cyber mission assurance plans and build confidence on the part of the unit in its ability to operate in the contested environment. Unfortunately, there is not a good method for integrating mission owners and their systems into the "cyber range" to properly exercise cyber mission assurance. In the end, the goal of exercising should be to reduce the

uncertainties of operating in the contested cyber environment and to think creatively in an attempt to break the plan to find gaps or solutions to known or unknown hard problems.

V. Conclusions and Recommendations

Cyber mission assurance is an important process when considering the vast amount of missions relying upon massive amounts of cyber assets for successful mission accomplishment that can be vastly different in regards to architecture and software applications. 24 AF has sought to formalize a concept of operations for tackling its mission of cyber mission assurance within its own resource constrained environment. Units have to realize that cyber mission assurance is not just a 24 AF problem but a unit (mission owner) and 24 AF problem. Units needs to proactively seek out 24 AF support through their appropriate MAJCOM or COCOM to start developing cyber mission assurance plans in order to reduce the unit's uncertainties of executing its mission in a contested cyber environment. Having a plan is just the beginning of assuring missions in cyberspace. To continue to reduce the uncertainties, the plan must be exercised in as much detail and in as realistic an environment as possible prior to trying to implement the plan in a wartime or contingency environment, not only by 24 AF but also by the mission owners themselves.

MAJCOMs need to take a vested interest in cyber mission assurance for their units as the MAJCOMs are the force providers to the COCOMs. MAJCOMs have the mission of training and equipping the units in support of a COCOM's needs. Mission assurance comes at a price to the unit and training is required to ensure the unit can operate in a cyber contested environment. Therefore, MAJCOMs will need to provide resources to units to meet the needs for cyber mission assurance. MAJCOMs will also be able to provide the consolidation needed by 24 AF for multiple units with the same or similar

mission sets and will also be able to create the bridge needed between the unit mission experts and the 24 AF's cyber mission assurance experts.

There also needs to be a continued emphasis on the part of the Air Force to look for and develop those individuals that can help bridge the gap between operations and cyber, thus improving cyber mission assurance. What is needed are individuals who not just understand how to operate their little piece of cyber but understand how cyber works. While the newest generations entering the Air Force have grown up in a cyber 'savvy' environment, these individuals may not necessarily understand the inner workings of how the cyber devices they are operating actually work, they just know the device works.

As for exercising mission assurance plans, red teams not only need to continue to stress the plans to point of breaking in an exercise but they also need to debrief the unit and those tasked with defending the cyber dependencies so as to create a learning environment. What is seen all too often is the unit gets beat up in an exercise but never gets a debrief on what was done in order for everyone to learn from the beating. The environment also needs to change for units in regards to how failure is perceived. If exercises are built around the premise of breaking the plan to find gaps or to figure out solutions to known hard problems, then the perception of failure needs not to be seen as necessarily bad but potentially good as lessons learned can lead to solutions found for discovered gaps or known hard problems that will lead to a higher potential for success in a combat environment. Units need to go into an exercise assuming there will be failure and be ready to do the analysis both real time and post exercise to develop and track lessons learned to solutions for later use.

This project is by no means the panacea that will solve all of the cyber mission assurance woes. Cyber mission assurance has several areas that are difficult problems and this research project deals with just one of those areas. Ideally, this research will stir thoughts and discussion at the unit level to look into their mission sets, determine their cyber dependencies and engage with 24 AF through the unit's MAJCOM or COCOM to begin handling its cyber mission assurance concerns. At the very least, if a unit runs through the outlined process, it will have deeper understanding of its missions and tasks as well as see how other outside agencies may affect the unit's mission. Lastly, as with any plan, the spelled out process may not entirely meet the needs of the unit and/or 24 AF and therefore may need modification to the specific situation in which the unit finds itself.

Future Research

As mentioned, this is just one small piece of cyber mission assurance. The following are areas for potential future research.

Research and develop technical solutions for generating the prioritized mission to cyber asset map.

Developing a technical solution was outside the expertise of the author. The process described in this paper could be improved with a technical solution that would provide a better and standardized way for capturing, organizing, correlating, and maintaining the data collected.

Research and development in methods for exercising cyber mission assurance plans all the way down to the mission owner or unit level.

This would prove beneficial to test the cyber mission assurance plans prior to having to use it in a real combat or contingency event.

Bibliography

24th Air Force. (2011 (DRAFT)). *DRAFT 24th Air Force & 624th Operations Center Mission Assurance Operating Concept.*

American Heritage Dictionary. (2011). Retrieved from http://www.ahdictionary.com

D'Amico, A., Buchanan, L., Goodall, J., & Walczak, P. (2010). Mission Impact of Cyber Events: Scenarios and Ontology to express the Relationships between Cyber Assets, Missions and Users. *The Proceedings of the 5th International Conference on Information Wafare and Security*, (pp. 388-397). Wright-Patterson AFB.

Department of Defense. (2006). *Information Operations, JP 3-13.* Washington: United States Department of Defense, Joint Chiefs of Staff.

Department of Defense. (2009). *DoD Architecture Framework Version 2.0, Volume 2: Architectural Data and Models.* Washington D.C.

Department of Defense. (2010). *DoD Policy and Responsibilities for Critical Infrastructure, DoDD 3020.40.* Washington: United States Department of Defense.

Department of Defense. (2011a). *Department of Defense Dictionary of Military and Associated Terms, JP 1-02.* Washington: United States Department of Defense, Joint Chiefs of Staff.

Department of Defense. (2011b). *Department of Defense Strategy for Operating in Cyberspace.* Washington: United States Department of Defense.

Department of Defense. (2011c). *Joint Publication 5-0 Joint Operation Planning.* Washington D.C.: Department of Defense, Joint Chiefs of Staff.

Department of the Air Force. (2010, July 15). *Cyberspace Operations, AFDD 3-12.* Washington: HQ USAF.

Department of the Air Force. (2011). *Air Force Basic Doctrine, AFDD 1.* Washington: HQ USAF.

Fortson, L., & Grimaila, M. (2007). Development of a Defensive Cyber Damage Assessment Framework. *Proceedings of the 2007 International Conference on Information Warfare and Security (ICIW 2007).* Monterey, CA: Naval Postgraduate School.

GAO. (1996). Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Washington: United States General Accounting Office.

Griffith, S. B. (1963). *Sun Tzu, The Art of War.* Oxford: Oxford University Press.

Grimaila, M. R., Mills, R. F., Haas, M., & Kelly, D. (2010). Mission Assurance: Issues and Challenges. *Security and Management*, (pp. 651-657).

Haigh, T., Harp, S., & Payne, C. (2010). AIMFIRST: Planning for Mission Assurance. *The Proceedings of the 5th International Conference on Information Warfare and Security*, (pp. 416-426). Wright-Patterson AFB.

International Organization for Standardization. (2009). *ISO 31000:2009 Risk Management - Principles and Guidelines.*

Jajodia, S., Ammann, P., & McCollum, C. D. (1999). Surviving Information Warfare. *IEEE Computer*, *32*(4), 57-63.

Lentz, R. F. (2009, May 5). Statement by Mr. Robert F. Lentz Deputy Assistant Secretary of Defense, for Cyber Identity and Information Assurance Before the U.S. House of Representatives Armed Services Committee Subcommittee on Terrorism, Unconventional Threats & Capability. Washington.

Military Operations Research Society. (2011a, March). *Mission Assurance: Analysis for Cyber Operations; Working Group III Outbrief.* Retrieved December 8, 2011, from Military Operations Research Society: http://www.mors.org/events/2011cyber.aspx

Military Operations Research Society. (2011b, March). *Synthesis Group Final Report.* Retrieved December 12, 2011, from http://www.mors.org/events/2011cyber.aspx

Moltke, H., & Hughes, D. J. (1995). *Moltke on the Art of War: Selected Writings.* Novato, CA: Presidio Press.

Pal, P., Rohloff, K., Atighetchi, M., & Schantz, R. (2010). Managed Mission Assurance - Concept, Methodology and Runtime Support. *IEEE Second International Conference on Social Computing* (pp. 1159-1164). Washington D.C.: IEEE Computer Society.

Pipkin, D. L. (2000). *Information Security, Protecting the Global Enterprise.* Upper Saddle River: Prentice Hall PTR.

Ware, W. (1970, February). Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security. Santa Monica, CA: The RAND Corporation.

Vita

Major Michael D. Pritchett graduated from Pittsburg High School in Pittsburg, Texas. He entered undergraduate studies at the University of North Texas in Denton, Texas where he graduated with a Bachelor of Arts degree in Computer Science and was commissioned through the Detachment 835 AFROTC in May 1998.

His first assignment was at Pensacola Naval Air Station, Florida as a student in Undergraduate Navigator Training in July 1998. In December 1999, Major Pritchett attended the B-52H Formal Training Unit. Upon completion of B-52 navigator training, he was assigned to the 23d Bomb Squadron, Minot AFB, North Dakota in September 2000. He deployed in support of Operation Enduring Freedom from January to May 2002 as a navigator, as well as Operation Iraqi Freedom from March to April 2003 and Operation Enduring Freedom from June to September 2003 as a radar navigator. Prior to leaving Minot, Major Pritchett also graduated from the United States Air Force Weapons School in December 2005 and from Touro University International with a Master of Business Administration in Information Technology Management in March 2006.

Major Pritchett's next assignment was to Barksdale AFB, Louisiana in December 2007 where he was an 11th Bomb Squadron Formal Training Unit Instructor and a 2d Operations Support Squadron Assistant Director of Operations. In June 2010, he was assigned to USSTRATCOM as the Chief of Aircraft Emergency Action Procedures. In May 2011, he entered the Graduate School of Engineering and Management, Air Force Institute of Technology. Upon graduation of the IDE Cyber Warfare program, he will be assigned to Air Force Global Strike Command.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
14-06-2012	Graduate Research Project	16 May 2011 – 15 June 2012

4. TITLE AND SUBTITLE
Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Pritchett, Michael D., Major

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
2950 Hobson Way, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/ICW/ENV/12-J01

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Colonel Robert Morris
Air Force Cyber Air Component Coordination Element
9800 Savage Mill Road
Suite 6477
Ft. George Meade, MD 20755
Robert.morris@us.af.mil; DSN 685-2866 Comm 240-373-2866

10. SPONSOR/MONITOR'S ACRONYM(S)
AFCYBER/ACCE

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT
Military organizations have embedded Information and Communication Technology (ICT), collectively known as "Cyberspace," into their core operational processes across all levels of military operations. Cyber mission assurance is an essential risk management activity focused on assuring an organization's mission capability in response to loss or degradation of cyber capabilities. The cyber mission assurance process requires an in depth analysis of the organization's mission including enumeration of its core mission processes, prioritization of mission processes, mapping of mission processes to underlying cyber capabilities, and application of control measures to mitigate risks to mission capability. Unfortunately, the structure of military organizations makes this type of analysis challenging as the mission tasks and cyber ICT capabilities always span multiple organizational boundaries.
The 24th Air Force recently developed new draft guidance for conducting cyber mission assurance. The goal of this research is to present a methodology enabling mission owners to efficiently prepare for cooperative cyber mission assurance engagements with 24th Air Force. The proposed methodology incorporates the new 24th Air Force guidance; best practices from commercial, governmental, and military organizations; and incorporates operational lessons learned. Application of the proposed methodology will enable more efficient and productive cyber mission assurance engagements with 24th Air Force.

15. SUBJECT TERMS
Cyber, mission assurance

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Michael R. Grimaila, PhD (ENV)
U	U	U	UU	56	**19b. TELEPHONE NUMBER** *(Include area code)* (937)257-3636x4800; michael.grimaila@afit.edu